Renée E. Rothauge, OSB #903712
MARKOWITZ HERBOLD PC
1211 SW Fifth Avenue, Suite 3000
Portland, Oregon 97204-3730
Telephone: (503) 295-3085
Fax: (503) 323-9105
reneerothauge@markowitzherbold.com

Michael J. Summersgill (*pro hac vice*)
Jordan L. Hirsch (pro hac vice)
WILMER CUTLER PICKERING HALE AND DORR LLP
60 State Street
Boston, Massachusetts 02109
Telephone: (617) 526-6000
Fax: (617) 526-5000
michael.summersgill@wilmerhale.com
jordan.hirsch@wilmerhale.com

Todd C. Zubler (*pro hac vice*)
WILMER CUTLER PICKERING HALE AND DORR LLP
1875 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
Telephone: (202) 663-6000
Fax: (202) 663-6363
todd.zubler@wilmerhale.com

Attorneys for Defendant and Counterclaim Plaintiff Intel Corporation

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION

FEREYDUN TABAIAN and AHMAD ASHRAFZADEH,

Plaintiffs,

v.

INTEL CORPORATION,

Defendant.

Case No. 3:18-cv-326-HZ

INTEL CORPORATION'S RESPONSE TO PLAINTIFFS' MOTION FOR ENTRY OF PROTECTIVE ORDER

TABLE OF CONTENTS

I. INTRODUCTION 1
II. FACTUAL BACKGROUND 5
A. Adequate Protective Order Protections Are Crucial To Protecting Intel's Microprocessor Business 5
B. Intel Has Worked Diligently to Negotiate the Protective Order and Produce Technical Information While the Parties Negotiated the Protective Order 7
III. ARGUMENT 8
A. Plaintiffs' Motion Should Be Denied Because Plaintiffs Failed To Comply with Local Rule 7-1(a) 9
B. The Protective Order Should Include Intel's Source Code Provisions—Not the Source Code Provisions Proposed by Plaintiffs 10
1. Intel's Source Code Should Be Maintained at the Offices of Intel's Counsel 11
2. Electronic Devices and Media Should Not Be Allowed in the Source Code Review Room 15
3. The Protective Order Should Restrict Printing of Source Code to What Is "Reasonably Necessary" 19
C. Mr. Ashrafzadeh Should Not Be Allowed to Access Intel's Highly-Confidential Information and Source Code Materials 21
D. The Prosecution Bar Should Include Plaintiffs' Alternative Definition of "Relevant Technology" 27
E. Plaintiffs' Attempt to Disclose Intel's Confidential and Highly Confidential Information to Undisclosed Experts Should be Rejected 30
IV. CONCLUSION 34

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Affinity Labs of Texas, LLC v. Samsung Electronica Co.,
2013 WL 12147667 (E.D. Tex. Oct. 29, 2013) 11, 12

Applied Signal Tech., Inc. v. Emerging Markets Commc'ns, Inc.,
2011 WL 197811 (N.D. Cal. Jan. 20, 2011) 27

Auto-Kaps, LLC v. Clorox Co.,
2016 WL 1122037 (E.D.N.Y. Mar. 22, 2016) 33

AVM Techs., LLC v. Intel Corp.,
1:15-cv-33, Dkt. 129 (D. Del. Dec. 8, 2015) (Ex. 12) 14

Cherdak v. Koko Fitclub, LLC,
2015 WL 1895992 (D. Mass. Apr. 27, 2015) 19

Coca-Cola Bottling Co. of Shreveport v. Coca-Cola Co.,
107 F.R.D. 288 (D. Del. 1985) 26

Codexis, Inc. v. EnzymeWorks, Inc.,
2017 WL 5992130 (N.D. Cal. Dec. 4, 2017) 26

Crumb v. Orthopedic Surgery Med. Grp.,
479 F. App'x 767 (9th Cir. 2012) 9

In re Deutsche Bank Trust Co. Ams.,
605 F.3d 1373 (Fed. Cir. 2010) 26

In re Dynetix Design Sols. Inc.,
473 F. App'x 896 (Fed. Cir. 2012) 12

EPL Holdings, LLC v. Apple Inc.,
2013 WL 2181584 (N.D. Cal. May 20, 2013) 16

Evans v. Jackson Cty.,
2015 WL 2170114 (D. Or. May 7, 2015) 9

GeoTag, Inc. v. Frontier Commc'ns Corp.,
2013 WL 12134192 (E.D. Tex. Jan. 8, 2013) 13, 17

Godo Kaisha IP Bridge 1 v. Intel Corporation,
2:17-cv-676, Dkt. 56 (E.D. Tex. March 5, 2018) (Ex. 9) 13, 17

Gray v. Geisel,
611 F. App'x 442 (9th Cir. 2015) 9

Hangartner v. Intel Corp.,
3:14-cv-141, Dkt. 68 (D. Or. July 17, 2014) (Ex. 11) 14, 31

I2Z Tech., LLC, v. Microsoft Corp.,
3:11-cv-1103, Dkt. 36 (D. Or. March 29, 2012) (Ex. 14) 14, 18, 21, 23, 32

IP Innovation L.L.C. v. Thomson, Inc.,
2004 WL 771233 (S.D. Ind. Apr. 8, 2004) 24

Layne Christensen Co. v. Purolite Co.,
271 F.R.D. 240 (D. Kan. 2010).....22

McDavid Knee Guard, Inc. v. Nike USA, Inc.,
2009 WL 1609395 (N.D. Ill. 2009) 22

Medina v. Microsoft Corp.,
2014 WL 3884506 (N.D. Cal. Aug. 7, 2014) 3, 23

Memory Integrity, LLC v. Intel Corporation,
3:15-cv-262, Dkt. 92 (D. Or. June 3, 2015) (Ex. 10).....13, 17, 31

Merit Industries v. Feuer,
201 F.R.D. 382, 384 (E.D. Pa. 2000).....26

In re Neubauer,
173 B.R. 505 (D. Md. 1994) 30

Novitaz, Inc. v. Shopkick, Inc.,
2015 WL 12966286 (N.D. Cal. Mar. 18, 2015).....16

OpenTV, Inc. v. Apple, Inc.,
2014 WL 5079343 (N.D. Cal. Oct. 9, 2014).....20

Oracle Corp. v. DrugLogic, Inc.,
2012 WL 2244305 (N.D. Cal. June 15, 2012) 32

Pellerin v. Honeywell Int'l Inc.,
2012 WL 112539 (S.D. Cal. Jan. 12, 2012).....33

Schlafly v. Public Key Partners,
94-cv-20512, Dkt. 74 (N.D. Cal. July 19, 1995) 25

SemCon Tech, LLC v. Intel Corp.,
3:13-cv-99, Dkt. 79 (D. Or. April 12, 2013) (Ex. 15).....18, 31

Shared Memory Graphics, LLC v. Apple, Inc.,
2010 WL 4704420 (N.D. Cal. Nov.12, 2010) 25

Smartflash LLC v. Apple Inc.,
2014 WL 10986995 (E.D. Tex. May 12, 2014).....20

Tailored Lighting, Inc. v. Osram Sylvania Prods., Inc.,
236 F.R.D. 146 (W.D.N.Y. 2006).....22, 26

Tehrani v. Polar Elecs. Inc.,
2006 WL 8435287 (C.D. Cal. Nov. 8, 2006).....22, 24

Telebuyer, LLC v. Amazon.com, Inc.,
2014 WL 5804334 (W.D. Wash. July 7, 2014) 11, 20, 25

Thompson ex rel. Thorp Family Charitable Remainder Unitrust v. Federico,
324 F. Supp. 2d 1152 (D. Or. 2004) 9

TVIIM, LLC v. McAfee, Inc.,
2014 WL 2768641 (N.D. Cal. June 18, 2014) 21

U.S. Steel Corp. v. United States,
730 F.2d 1465 (Fed. Cir. 1984).....25

Unwired Planet LLC v. Apple Inc.,
2013 WL 1501489 (D. Nev. Apr. 11, 2013).....20

Verinata Health, Inc. v. Ariosa Diagnostics, Inc.,
2013 WL 5663434 (N.D. Cal. Oct. 17, 2013).....13

Walker Digital, LLC v. Fandango, Inc. et. al.,
1:11-cv-313, Dkt. 88 (D. Del. Feb. 14, 2012) (Ex. 13).....14, 18, 21, 23, 31

Wreal LLC v. Amazon.com, Inc.,
2014 WL 7273852 (S.D. Fla. Dec. 19, 2014) 30

Rules

D. Oregon Local Rule 7-1 .....1, 2, 9

I. INTRODUCTION

Plaintiffs had no basis to file their Motion for Protective Order (Dkt. 65). Plaintiffs failed to properly meet and confer as required by the Local Rules and, as a result, moved for relief on multiple issues that are no longer in dispute. Moreover, Plaintiffs propose highly unusual Protective Order provisions that risk irreparable harm to Intel's business and that are directly contrary to the Northern District of California Model Order, well-established case law (including precedent in this District), and ***the protective orders that Plaintiffs' own counsel have entered when representing other clients.*** Plaintiffs' motion should be denied and Intel's proposed Protective Order (attached as Exhibit 1) should be entered for five primary reasons.

First, Plaintiffs filed their motion without properly meeting and conferring as required by Local Rule 7-1(a). After having waited two weeks to respond to one of Intel's Protective Order proposals, and more than a week to respond to Intel's proposal to use the N.D. Cal. Model Order as the basis for the Protective Order, Plaintiffs demanded that Intel meet and confer within 48 hours of receiving Plaintiffs' latest proposed protective order. Even though counsel for Intel explained that they needed to first discuss Plaintiffs' proposal with in-house Intel counsel and proposed conferring with Plaintiffs the following day (*i.e.*, within 72 hours of receiving Plaintiffs' proposal), Plaintiffs refused to wait and filed their motion without a meet-and-confer. Had they met and conferred, Plaintiffs would have learned that ***there is no longer any dispute on many of the provisions that Plaintiffs raised in their motion.*** Indeed, there are only ***four*** provisions (not six, as Plaintiffs allege) in dispute: (1) the protections for Intel's highly sensitive source code; (2) whether named plaintiff Ahmad Ashrafzadeh should be allowed access to Intel's highly confidential information; (3) the definition of "Relevant Technology" subject to the

"prosecution bar"; and (4) whether the Protective Order should include a standard provision requiring the parties to identify experts to whom they intend to disclose the other side's confidential or highly confidential material. Plaintiffs' failure to properly meet and confer violates Local Rule 7-1 and warrants denial of Plaintiffs' motion.

Second, Plaintiffs propose dangerous and highly unusual provisions relating to Intel's sensitive source code that would put Intel's code at high risk of inadvertent disclosure and that are directly contrary to the N.D. Cal. Model Order, long-established case law, and their own counsel's established practice. Intel's source code is not generic source code—it is specially designed code that is the result of years and billions of dollars of research of development and that is the blueprint for billions of dollars of industry-leading Intel products. Intel's source code sets forth the detailed operations and functions of the Intel products at issue in this case and could be used to make exact copies of the Intel products. Third parties, including foreign governments, have tried repeatedly to steal Intel's source code and inadvertent disclosure would significantly increase the risk that these third parties succeed in obtaining Intel's code. Nonetheless, Plaintiffs' proposed order deviates from well-accepted practice on this subject and increases the chances of inadvertent disclosure by: (1) requiring Intel to produce its source code ***at locations maintained by Plaintiffs***, preventing Intel from securing and monitoring how the code is accessed or who accesses it; (2) ***permitting Plaintiffs to bring copying equipment*** into the room that contains Intel's source code; and (3) not providing ***any limit*** on the amount of source code that Plaintiffs can print. Plaintiffs' counsel have rightfully rejected these provisions—and obtained the source code protections Intel requests here—when representing other clients in the past. Intel's proposal brings the Protective Order in line with the N.D. Cal.

Model Order, established patent practice, and Protective Orders entered in cases similar to this one.

Third, Plaintiffs' proposal takes the extreme position that one of the named Plaintiffs in this case—Ahmad Ashrafzadeh—should be permitted access to all of Intel's highly confidential information, including technical documents and source code. This also is directly contrary to well-established patent practice, the N.D. Cal. Model Order, and Plaintiffs' counsel's own practices when representing other clients. Disclosure of Intel's highly confidential information to Mr. Ashrafzadeh is particularly inappropriate because Plaintiffs concede that Mr. Ashrafzadeh is involved in patent licensing and is currently pursuing patents relating to microprocessor technology. Ex. 5 at 1 (July 18 Email from McAndrew to Coviello). Courts have repeatedly held in these circumstances that the risk the plaintiff would use the defendant's highly sensitive information in licensing discussions, to file new lawsuits, or to draft new patent claims precludes access to any of the defendant's highly confidential information. *See Medina v. Microsoft Corp.*, 2014 WL 3884506, at *3 (N.D. Cal. Aug. 7, 2014) ("As Dr. Medina is the opposing litigant, he may not view Microsoft's highly confidential information.").

Fourth, Plaintiffs' prosecution bar proposal is flawed. The prosecution bar states that attorneys who access highly confidential information produced by the other side cannot draft or prosecute patent applications relating to specifically defined "Relevant Technology" for a period of time. Prosecution bars are necessary to prevent patent attorneys from using (intentionally or inadvertently) highly sensitive technical information produced by an opposing party to draft patent claims for another client. Plaintiffs do not dispute that a prosecution bar is appropriate in this case. But they propose two competing definitions of the "Relevant Technology" subject to

the bar: a first definition and an "alternative definition." Plaintiffs' first definition of "Relevant Technology"—"the use of calibration to improve the performance characteristics of voltage regulator circuits for powering integrated circuit and microprocessor chips"—is far too narrow. Plaintiffs have already taken the position that the asserted patent relates to more than "the use of calibration" and have demanded that Intel produce documents regarding power regulation generally, beyond any alleged "use of calibration." Plaintiffs' first proposed definition of "Relevant Technology" would thus allow Plaintiffs' counsel to review Intel's highly confidential power regulation information and continue to prosecute patent applications relating to power regulation—the very thing the prosecution bar is designed to prevent. Instead, the definition of "Relevant Technology" should correspond to the scope of Intel information that Plaintiffs are demanding and receiving. Intel submits that Plaintiffs' "alternative definition" of "Relevant Technology"—"circuits for regulating power in microprocessors or other integrated logic circuits" (Dkt. 65 at 8 n.3)—is consistent with the scope of the Intel information Plaintiffs' counsel have demanded in this case and gives the prosecution bar appropriate scope.

Finally, Plaintiffs attempt to eliminate the standard Protective Order requirement that any party wishing to disclose the other side's confidential or highly confidential information to an expert must first disclose the expert and give the other side an opportunity to object to the expert. This is directly contrary to well-established case law, the Protective Orders of similar cases, and the prior practice of Plaintiffs' own counsel.

II. FACTUAL BACKGROUND

A. Adequate Protective Order Protections Are Crucial To Protecting Intel's Microprocessor Business

Plaintiffs have requested production of Intel's most sensitive and technical product information. The source code, schematics, layout files, and other highly sensitive technical information (collectively "source code materials") that Intel is producing in this case is not generic source code that is used across an industry or is publicly available. Instead, it contains Intel's "crown jewels"—the trade secrets and technical information that could be used to make exact copies of Intel's microprocessors. As explained in the accompanying Declaration of David Papworth, Intel's Director of Microprocessor Product Development and an Intel Fellow, the importance and confidential nature of this information cannot be overstated:

- Intel's source code materials provide the "blueprint" for Intel's products. Source code sets out the detailed operation of Intel's products—it describes every operation and function of Intel's microprocessors. Papworth Decl. ¶¶ 5, 8. Schematics and layout files provide the detailed layout and circuitry of the processors. *Id*. The source code materials contain the technical details that have given Intel its competitive advantage in the microprocessor industry. *Id.* at ¶¶ 9, 13.
- Intel has devoted years of research and development and billions of dollars to develop the source code materials. They are Intel's most prized and confidential information. *Id.* at ¶¶ 7, 10, 15-16, 18.
- Companies or entities that obtain copies of Intel's source code materials could make copies of Intel's products with relative ease. *Id.* at ¶ 11.

- For that reason, Intel restricts access to source code information even within Intel itself. Only employees with a "need to know" have access to Intel's source code materials. Source code materials are maintained on a secure network that is monitored by a file system administrator who manages access on an individual-by-individual basis. Only certain engineers directly involved with creating Intel's source code materials can be granted access. *Id.* at ¶ 18.
- Disclosure of all or even portions of Intel's highly sensitive source code information could be devastating to Intel's business. Any copies or knockoffs made using Intel's source code materials would include the unique features that Intel designed and developed at enormous expense and that are responsible for Intel's competitive advantage. This would cause irreparable harm to Intel's business, putting billions of dollars at risk. *Id.* at ¶¶ 15-16.
- Third parties, including foreign governments, have tried repeatedly to steal Intel's source code. *Id.* at ¶ 17. Indeed, a 2018 report by the U.S. National Counterintelligence and Security Center ("NCSC Report"), explained that foreign agents have directly targeted Intel and other U.S. companies. Ex. 6 (NCSC Report) at 7.
- Once source code materials and other highly confidential technical information are out of Intel's control, Intel cannot ensure that the information is not copied or transmitted electronically. Even one inadvertent email or file transfer could cause irreparable competitive harm to Intel. Papworth Decl. ¶ 16.

The dispute over the Protective Order, in other words, is extremely high-stakes for Intel. Given the importance of Intel's confidential information and the risks of disclosure, it is critical for Intel that the Protective Order contain sufficient protections for Intel's highly confidential technical information.

B. Intel Has Worked Diligently to Negotiate the Protective Order and Produce Technical Information While the Parties Negotiated the Protective Order

Because of the importance of the Protective Order to Intel's business, Intel submits that the dispute over the Protective Order should focus on the merits of the provisions at issue and the need to adequately protect Intel's most sensitive information—not allegations of improper conduct. That said, Intel is compelled to once again correct Plaintiffs' misstatements regarding the history of the parties' protective order negotiations. Plaintiffs' suggestion that Intel refused to negotiate a Protective Order (Dkt. 65 at 3) and somehow tried to use the negotiations to "forestall" discovery (*id.* at 4) could not be further from the truth. Intel has proposed multiple protective order drafts—(1) an initial draft on May 25, 2018; (2) a proposed interim Protective Order on July 12, 2018; and (3) a compromise proposal based on the N.D. Cal Model Order on July 23, 2018—and based on the specific circumstances of this case, Intel has compromised substantially in order to eliminate unnecessary motion practice and expedite this litigation. Intel also has already produced a substantial volume of technical documentation under the interim Protective Order (Dkt. 54) while the parties have negotiated the Protective Order. Among other things, Intel has already produced more than 2,000 technical documents, has made available for inspection source code materials for Intel's products, has presented for deposition the lead designer of the FIVR technology at issue in this case, and has accommodated each and every one

of Plaintiffs' requests to inspect and print Intel's source code materials (Plaintiffs have already inspected Intel's code for seven days). Plaintiffs' assertion that Intel is using the Protective Order to forestall discovery is belied by the fact that Plaintiffs have had access to Intel's production under the Interim Protective Order. The parties' failure to reach agreement on the Protective Order is thus not a result of any attempt to forestall discovery. Instead, the parties have not reached an agreement because Plaintiffs have insisted on highly unusual and dangerous provisions that would place Intel's most sensitive information at risk and risks irreparable competitive harm to Intel's business.[1]

III. ARGUMENT

Intel's proposed protective order, which closely tracks the N.D. Cal. Model Order, should be entered for four reasons.

[1] Plaintiffs also are attempting to use the protective order dispute as an excuse to extend their deadline to submit infringement contentions (currently due August 13). But no such stay of the case schedule is warranted. Intel has produced a substantial number of technical documents—as well as source code materials including schematics and other design files—that show in detail the features and functionality of FIVR and the accused products. Plaintiffs have had access to these materials under the interim protective order, and they have taken advantage of that access by reviewing the source code for six days and by using many of the Intel documents at a technically detailed deposition of Intel's lead FIVR designer. If some of Plaintiffs' legal team has chosen not to review Intel materials because of the prosecution bar in the interim protective order, that was their choice; the prosecution bar provision was readily apparent when Plaintiffs voluntarily chose to stipulate to the interim order with their deadline for infringement contentions pending in the near future. Particularly after the deposition of Intel's lead FIVR designer, Intel does not believe Plaintiffs have any basis to maintain this lawsuit. Intel is entitled to see Plaintiffs' infringement contentions now, so Intel can prepare its defense and seek resolution of this case at the earliest opportunity.

A. Plaintiffs' Motion Should Be Denied Because Plaintiffs Failed To Comply with Local Rule 7-1(a)

After Intel proposed a draft Protective Order on May 25, 2018. Plaintiffs waited two weeks to provide any proposed edits or counterproposals. Plaintiffs then waited over a week to provide a responsive proposal to Intel's July 23, 2018 proposed order. Yet when Plaintiffs provided their proposed order on the evening of July 31, 2018, they demanded that Intel meet and confer by August 2—***less than 48 hours later***. Ex. 7 at 4 (July 31 Email from McAndrew to Coviello). Intel's counsel explained that they needed to discuss the proposal with in-house Intel counsel and thus could not confer with Plaintiffs within the proposed 48-hour timeframe—but offered to confer the very next day. *Id*. at 3 (August 1 Email from Coviello to McAndrew). Plaintiffs ignored that request and filed their motion on August 2 without any meet-and-confer on their latest proposal. *Id.* at 1 (August 2 Email from McAndrew to Coviello). As a result, Plaintiffs moved on multiple issues—including procedures for designating sensitive material, what party has the burden when objecting to experts, and the process for the inadvertent production of material—that are not in dispute. Intel's counsel would have told Plaintiffs during a meet-and-confer that, after internal discussion, Intel can agree to Plaintiffs' proposals on each of these provisions.

Plaintiffs' failure to meet and confer as required by the Local Rules warrants denial of their motion. *See Gray v. Geisel*, 611 F. App'x 442, 443 (9th Cir. 2015) (nonprecedential) ("The district court did not abuse its discretion in denying Gray's motion to compel discovery on the basis of her failure to comply with the local 'meet and confer' rule."); *Crumb v. Orthopedic Surgery Med. Grp.*, 479 F. App'x 767 (9th Cir. 2012) (same) (nonprecedential); *Thompson ex*

rel. Thorp Family Charitable Remainder Unitrust v. Federico, 324 F. Supp. 2d 1152, 1172 (D. Or. 2004) ("[T]he court believes it is appropriate to deny plaintiff's motion for failure to comply with the Local Rules' meet-and-confer provision."); *Evans v. Jackson Cty.*, 2015 WL 2170114, at *3 (D. Or. May 7, 2015) (noting that local rules on meeting and conferring "makes no exception for parties who have struggled to work together in the past. Defendants violated this requirement when they filed their motion for summary judgment without attempting to discuss its contents with Plaintiff. This failure alone is sufficient grounds to deny Defendants' motion for summary judgment.").

B. The Protective Order Should Include Intel's Source Code Provisions—Not the Source Code Provisions Proposed by Plaintiffs

Plaintiffs' proposed Protective Order includes highly unusual source code provisions that do not come close to sufficiently protecting Intel's code. Plaintiffs' proposals significantly increase the risk of inadvertent disclosure of Intel's source code and, as a result, irreparable harm to Intel's business. The parties dispute three source code provisions: whether the code should be produced at the offices of Plaintiffs' counsel or Intel's counsel; whether copying equipment should be permitted in the source code room; and whether there should be a "reasonable" limit on the number of pages of source code the Plaintiffs may print. In each instance, Intel has proposed provisions that are necessary to minimize the risk of copying or inadvertent disclosure of Intel's source code and that are consistent with the N.D. Cal. Model Order, case law from around the country, Intel's practices in other patent litigations, and Plaintiffs' counsel's own practices in other cases.

1. Intel's Source Code Should Be Maintained at the Offices of Intel's Counsel

Intel's proposed Protective Order allows Intel to maintain control over its source code and produce it at the offices of Intel's counsel in Portland (where Plaintiffs filed this case and where Plaintiffs' counsel also have offices). Ex. 1, ¶ 9(c). Plaintiffs' proposal removes any control Intel has over its source code and requires Intel to make source code available at the offices of Plaintiffs' counsel and Plaintiffs' experts. (Dkt. 65-1) (Plaintiffs' Proposed Protective Order), ¶ 9(c); Ex. 2 (Comparison of Plaintiffs' Protective Order to Intel's Protective Order), ¶ 9(c). Intel's proposal should be adopted for multiple reasons.

First, Intel's proposal minimizes the risk of inadvertent disclosure of Intel's source code. As explained above and in Mr. Papworth's declaration, even one inadvertent email or keystroke could expose Intel's source code to public disclosure, hacking, or theft and cause irreparable harm to Intel's microprocessor business. Papworth Decl. ¶¶ 14, 16. As Intel has documented in its securities filings with the SEC, Intel is "a target of malicious attackers who attempt to gain access to our network or data centers or those of our customers or end users" and "steal proprietary information related to our business, products, employees, and customers." Ex. 8 (2017 Intel Corporation 10-K) at 49. By limiting the production of source code to the offices of Intel's counsel, Intel's proposal allows Intel to maintain control over the code and minimize the risks of inadvertent disclosure. Intel can ensure that only authorized individuals access the code using authorized equipment, that the room containing the code is properly secured at all times, and that the code is properly handled. *See Affinity Labs of Texas, LLC v. Samsung Electronica Co.*, 2013 WL 12147667, at *2 (E.D. Tex. Oct. 29, 2013) ("Given the highly confidential nature

of source code, Defendants are justified in not wanting the source code housed anywhere other than their outside counsels' offices."); *Telebuyer, LLC v. Amazon.com, Inc.*, 2014 WL 5804334, at *2 (W.D. Wash. July 7, 2014) (granting motion to supplement protective order with source code protections because "[t]he proposed source code provision is designed not only to hold the designated parties to their word, but also to prevent any others from gaining unauthorized access to the information. It restricts how, when, and where the information is displayed, how much can be printed, and how it is transported. … Telebuyer's promise of fidelity to the confidentiality rules, however sincere, is not a substitute").

Second, Intel's proposal comes directly from the N.D. Cal. Model Order. Recognizing the sensitivity of source code, the N.D. Cal. Model Order specifically states that source code will be produced in the offices of the ***producing party's*** counsel. Ex. 4 (N.D. Cal. Model Order), ¶ 9(c) ("Any source code produced in discovery shall be made available for inspection, in a format allowing it to be reasonably reviewed and searched, during normal business hours or at other mutually agreeable times, at an office of the Producing Party's counsel or another mutually agreed upon location.").

Third, courts around the country also have recognized the sensitivity of source code and have explicitly held that the party producing source code should be permitted to maintain control over the code by limiting production to the offices of its counsel. *See In re Dynetix Design Sols. Inc.*, 473 F. App'x 896, 896 (Fed. Cir. 2012) (nonprecedential) (denying mandamus relief predicated on argument that "restrictions were too burdensome" in Model Order of "Northern District of California, which … makes produced source code available for inspection only at the office of the producing party's counsel during business hours, unless the parties otherwise agree,

and prohibits the receiving party from transferring the source code onto a recordable device"); *Affinity Labs of Texas.*, 2013 WL 12147667, at *2 ("Given the highly confidential nature of source code, Defendants are justified in not wanting the source code housed anywhere other than their outside counsels' offices."); *Verinata Health, Inc. v. Ariosa Diagnostics, Inc.*, 2013 WL 5663434, at *1–2 (N.D. Cal. Oct. 17, 2013) (denying request to require defendant to produce its source code outside of its counsel's office); *GeoTag, Inc. v. Frontier Commc'ns Corp.*, 2013 WL 12134192, at *2 (E.D. Tex. Jan. 8, 2013) ("The Court believes it is reasonable for Defendants to provide source code at the office of the producing party or where it is kept in the ordinary course of business. *See* Fed. R. Civ. P. 34(b)(2)(E)(i). Shifting the travel burden from Plaintiff to Defendants is unwarranted in this action."). Indeed, Plaintiffs ***do not cite a single case*** in which a court found that a party's source code must be produced the offices of the opposing party. *See* (Dkt. 65) (Plaintiffs' Motion for Entry of Reasonable Protective Order) at 9-11.

Fourth, Intel's proposal is consistent with source code provisions in protective orders entered in prior cases in which Intel was a defendant—including cases in this District. This court and courts around the country have recognized that, because of the sensitivity of Intel's source code, Intel should be permitted to maintain control over the code by making it available at the offices of Intel's counsel. *See Godo Kaisha IP Bridge 1 v. Intel Corporation*, 2:17-cv-676, Dkt. 56 at 7 (E.D. Tex. March 5, 2018) (protective order provides that "[T]he stand-alone computer(s) may o***nly be located at the offices of the producing Party's outside counsel*** in the United States, unless the producing and receiving parties mutually agree otherwise." (emphasis added)) (Ex. 9); *Memory Integrity, LLC v. Intel Corporation*, 3:15-cv-262, Dkt. 92 at 14 (D. Or. June 3, 2015) (protective order provides that "Source Code shall be made available for inspection in electronic

format ***at the office of the Producing Party's Outside Counsel***." (emphasis added)) (Ex. 10); *Hangartner v. Intel Corp.*, 3:14-cv-141, Dkt. 68 at 12 (D. Or. July 17, 2014) (protective order states that "Confidential information shall only be provided to persons authorized to receive Source Code -Outside Counsels' Eyes Only - Restricted Confidential information and only on a 'stand-alone' computer … at a secure location at the selection of the Receiving Party of either the Portland, Oregon or Seattle, Washington ***office of the Producing Party's counsel***." (emphasis added)) (Ex. 11); *AVM Techs., LLC v. Intel Corp.*, 1:15-cv-33, Dkt. 129 at 10 (D. Del. Dec. 8, 2015) (protective order provides that "One of the Secured Computers shall be made available ***in the offices of the Producing Party's Outside Counsel*** in Washington, D.C., and the other shall be made available in the Wilmington, Delaware office of the Producing Party's Outside Counsel." (emphasis added)) (Ex. 12).

Fifth, in prior cases, Plaintiffs' own counsel has insisted on ***the same protections that Intel now proposes***. In multiple instances in the past, Plaintiffs' counsel have demanded that source code produced by their clients be made available only in their offices—not the offices of the opposing party. *See Walker Digital LLC, v. Fandango, Inc. et. al.*, 1:11-cv-313, Dkt. 88 at 3 (D. Del. Feb. 14, 2012) (Klarquist Sparkman, LLP – Jeffrey Love) ("Any source code that is produced in this case shall be made available for inspection in electronic (*e.g.*, native) format at an office of Producing Party's counsel, or at a mutually agreeable location.") (Ex. 13); *I2Z Tech., LLC, v. Microsoft Corp.*, 3:11-cv-1103, Dkt. 36 (D. Or. March 29, 2012) (Klarquist Sparkman, LLP – John Vandenberg) (same) (Ex. 14).

Finally, the balance of interests favors Intel's proposal. Plaintiffs complain that under Intel's proposal, Plaintiffs' experts would have to travel to the offices of Intel's counsel in

Oregon to review code. (Dkt. 65 at 10). As an initial matter, it is hardly a burden for Plaintiffs' lawyers to have to travel to the jurisdiction where they chose to file this case. Indeed, Plaintiffs have already inspected Intel's code for seven days and are coming back for more days of review this week. Moreover, Intel's proposal does not cause any greater inconvenience to Plaintiffs' experts than to Intel's. Intel's experts will operate under the same conditions—just like Plaintiffs, Intel's experts can review source code only at the offices of Intel's counsel. Conversely, Plaintiffs' proposal presents potentially catastrophic harm to Intel. A single mistake—one unauthorized access or inadvertent disclosure—could expose Intel's "crown jewels" to the public or a competitor and cause irreparable harm to Intel's business. This dwarfs any alleged inconvenience to Plaintiffs of traveling to review Intel's code.

2. Electronic Devices and Media Should Not Be Allowed in the Source Code Review Room

Intel's proposed Protective Order prohibits Plaintiffs from using, during the inspection of Intel's source code, any electronic device or media that could be used to copy Intel's code. Ex. 1, ¶ 9(c). Plaintiffs' proposal, on the other hand, would allow Plaintiffs to bring laptops, cameras, phones, external media such as flash drives and hard drives, and other electronic devices into the room that contains Intel's source code. (Dkt. 65-1, ¶ 9(c)); Ex. 2, ¶ 9(c). Intel's proposal should again be adopted for multiple reasons.

First, Intel's proposal is necessary to minimize the risk of intentional or inadvertent copying or disclosure of Intel's source code. Allowing copying equipment into the room that contains Intel's source code significantly increases the risk of inadvertent disclosure—laptops used to take notes of Intel's code could be misplaced, electronic files containing notes of Intel's

code could be inadvertently transferred or emailed, pictures of Intel's code could be mistakenly distributed, external media containing files relating to Intel's code could be lost or distributed in error. A single one of these events could cause catastrophic harm to Intel. Further, allowing copying equipment increases the risk of theft by third parties. As Mr. Papworth explains, Intel's source code has been targeted by attempted cyberattacks and cyberthefts in the past. Papworth Decl. ¶17. Hackers can attempt to access Intel's source code in many ways, including by accessing any electronic devices that have been used in close proximity to the code, *id.* ¶17:

- A hacker can access a laptop that is carried into the source code room and used to take notes from the source code review;
- A hacker can access a camera or phone that is used to take pictures of code;
- A hacker can access external media (flash drives, hard drives, etc.) that contain the code or notes relating to the code.

Intel's proposal minimizes each of these risks. Under Intel's proposed Protective Order, reviewers can take notes on paper but cannot bring any electronic devices that can be used for copying into the source code room. Ex. 1 at ¶ 9(c).

Second, it is standard in patent cases to prohibit electronic devices in the room that contains source code. Courts have repeatedly held that because of the highly confidential nature of source code, copying devices should be prohibited. *See Novitaz, Inc. v. Shopkick, Inc.*, 2015 WL 12966286, at *2 (N.D. Cal. Mar. 18, 2015) ("[S]ource code protective orders routinely entered in this Court provide that use of electronic devices, such as laptops and cell phones, is prohibited while accessing the source code."); *EPL Holdings, LLC v. Apple Inc.*, 2013 WL 2181584, at *6 (N.D. Cal. May 20, 2013) ("The Court accordingly finds that Apple's proposed

ban on cellphones and other similar devices is reasonable."); *GeoTag*, 2013 WL 12134192, at *3 ("The Court is unconvinced that sufficient review of Defendants' source code requires a cellular telephone or note-taking computer. In light of the highly confidential nature of the source code, allowing these devices within the secure room would significantly increase the possibility of inadvertent disclosure. Plaintiff has not shown any necessity for these devices. In this instance, the interest of protecting the source code far outweighs the convenience of allowing a cellular telephone or note-taking computing within the secure source code room."). Indeed, Plaintiffs fail to cite any cases supporting their proposal to bring copying devices into the source code room.

Third, Intel's proposal is consistent with the N.D. Cal. requirement that "the Receiving Party shall not copy, remove, or otherwise transfer any portion of the source onto any recordable media or recordable device." Ex. 4 at ¶ 9(b).

Fourth, Intel's proposal has been adopted in multiple prior litigations in which Intel has been involved, including one case in this District before Judge Simon and one case before Judge Hubel. *See Memory Integrity LLC v. Intel Corp.*, 3:15-cv-261, Dkt. 92 at 16-17 (D. Or. June 3, 2015) (protective order provides that "The Receiving Party is prohibited from bringing recordable media or recordable devices, including without limitation sound recorders, computers, cellular telephones, peripheral equipment, cameras, CDs, DVDs, or drives of any kind [into the] Source Code Review Room," and providing that "all [] notes will be taken on bound (spiral or other type of permanently bound) notebooks"); *Godo Kaisha IP Bridge 1 v. Intel Corp.*, 2:17-cv-676, Dkt. 56 at 7 (E.D. Tex. March 5, 2018) (protective order provides that "Except as otherwise provided herein, no electronic devices, including but not limited to laptops, cellular phones, PDAs, cameras, and voice recorders will be permitted in the secure location in which the Source

Code Material is inspected.") (Ex. 9); *SemCon Tech, LLC v. Intel Corp.*, 3:13-cv-99, Dkt. 79 at 7 (D. Or. April 12, 2013) (protective order provides that "[T]he Receiving Party shall not be permitted to bring electronic devices, including but not limited to laptops, hard drives, cellular phones, PDAs, cameras, and voice recorders, into the location of the Secure Computer.") (Ex. 15).

Fifth, Plaintiffs' proposal is again directly contrary to the positions their own counsel has taken in prior cases. When representing defendants, Plaintiffs' counsel have repeatedly insisted on provisions that preclude any electronic devices in the source code room—***the same protection that Intel now proposes***. *See Walker Digital, LLC v. Fandango, Inc. et. al.*, 1:11-cv-313, Dkt. 88 at 4 (D. Del. Feb. 14, 2012) (Klarquist Sparkman, LLP – Jeffrey Love) (protective order provides that "The Receiving Party may not take any form of camera, computer, computer storage device, or smartphone into the source code viewing room.") (Ex. 13); *I2Z Tech., LLC, v. Microsoft Corp.*, 3:11-cv-1103, Dkt. 36 at 27 (D. Or. March 29, 2012) (Klarquist Sparkman, LLP – John Vandenberg) (protective order provides that "The Receiving Party may not take any form of camera, computer, computer storage device, or mobile telephone into the source code viewing room…. The Receiving Party's outside counsel and/or Experts shall be entitled to take handwritten notes relating to the source code.") (Ex. 14).

Finally, the balance of interests again favors Intel's proposal. Plaintiffs' only purported justification for allowing electronic devices in the source code room is the desire to "take notes" on a laptop. (Dkt. 65 at 11.) But under Intel's proposal Plaintiffs and their experts can take notes in hard copy. The risk that Plaintiffs' proposal presents to Intel, on the other hand, is potentially devastating. If even a single page of notes on a laptop, a single picture from cell

phone, or single file on external media is hacked, inadvertently transferred, or stolen, Intel's business could be irreparably harmed.

3. The Protective Order Should Restrict Printing of Source Code to What Is "Reasonably Necessary"

As provided in the N.D. Cal Model Order, Intel proposes to limit the printing of source code to what is "reasonably necessary for the preparation of court filings, pleadings, expert reports, or other papers, or for deposition or trial." Ex. 1, ¶ 9(d). Plaintiffs' proposed protective order, on the other hand, has no limitation on the amount of Intel's source code that may be printed and would allow Plaintiffs to print the entire source code for Intel's products. Again, Intel's proposal should be adopted for multiple reasons.

First, Intel's proposal is necessary to minimize the risk that Intel's source code is copied and used to cause irreparable harm to Intel's business. Without any limitations on the amount of code that is printed, Plaintiffs could print the entire code for an Intel product. If these copies—or even a portion of them—are misplaced, lost, or stolen, entire products or features could be copied wholesale.

Second, Intel proposes the ***exact language*** from the N.D. Cal. Model Order. The Model Order recognizes that source code printing should be limited to what is "reasonably necessary" and the parties can bring any disputes over what meets this requirement to the court's attention. Ex. 4 N.D. Cal. Model Protective Order, ¶ 9(d).

Third, Intel's proposal is supported by precedent from around the country. In fact, courts have often imposed much ***stricter*** printing limitations than what Intel proposes, limiting the plaintiff to specific page and line limits. *See e.g.*, *Cherdak v. Koko Fitclub, LLC*, 2015 WL

1895992, at *3 (D. Mass. Apr. 27, 2015) ("The defendants proposed further that printing shall be limited to 25 pages of a continuous block of Source Code unless the Receiving Party meets its burden of demonstrating the need for additional pages…. While the plaintiff has stricken this page limit, this court finds it reasonable. It sets a presumptive limit while allowing the Receiving Party to prove that it needs more. The page limit is appropriately included."); *Smartflash LLC v. Apple Inc.*, 2014 WL 10986995, at *2 (E.D. Tex. May 12, 2014) ("Smartflash has offered no competing page limit proposal for printing source code. Given the highly sensitive nature of source code, there is good cause for some restrictions on printing. Defendants' proposal for a limit of 40 continuous pages is adopted."); *Unwired Planet LLC v. Apple Inc.*, 2013 WL 1501489, at *7 (D. Nev. Apr. 11, 2013) ("The court finds that Apple has established good cause to limit the amount of source code that Unwired may print beyond that which is 'reasonable.' Having considered the parties' positions, the court orders that Unwired shall be limited to printing 250 pages of source code and thirty continuous pages."); *Telebuyer*, 2014 WL 5804334, at *3 ("Amazon proposes a 25–page limit on printing of 'any continuous block of Source Code' …. Amazon also proposes a 1500-page aggregate printing limit …. These requirements appear reasonable. The receiving party still has the option to request more than 25 continuous pages when necessary to print a function or method in its entirety, and the parties are obligated to meet and confer in the event of a dispute concerning the print limitation.").[2] Once again, Plaintiffs have cited no case law supporting its position that there should be no reasonable limitation on printing source code.

[2] *See also OpenTV, Inc. v. Apple, Inc.*, 2014 WL 5079343, at *2 (N.D. Cal. Oct. 9, 2014) (holding that, instead of line limitations, "[t]he parties may print portions of source code, as is reasonably necessary, consistent with Paragraph 9(d) of the model protective order.").

Fourth, when representing other clients, Plaintiffs' own lawyers have agreed that source code printing should be limited. *See Walker Digital, LLC v. Fandango, Inc. et. al.*, 1:11-cv-313, Dkt. 88 at 7 (D. Del. Feb. 14, 2012) (Klarquist Sparkman, LLP – Jeffrey Love) (protective order limits source code printing to 35 pages of continuous text and 350 pages in aggregate) (Ex. 13); *I2Z Tech., LLC, v. Microsoft Corp.*, 3:11-cv-1103, Dkt. 37 at 22-23 (Klarquist Sparkman, LLP – John Vandenberg) (same) (Ex. 14).

Finally, the balance of interests again is overwhelmingly in Intel's favor. Plaintiffs have not articulated any reason they need to print more than the code that is reasonably necessary for their case. Intel, on the other hand, has significant need for its proposal—without a limitation on the number of printed source code pages, the risk of theft or inadvertent disclosure of the source code increases thereby risking irreparable harm to Intel's business.

C. Mr. Ashrafzadeh Should Not Be Allowed to Access Intel's Highly-Confidential Information and Source Code Materials

Plaintiffs' proposed Protective Order would allow a named Plaintiff in this case—Ahmad Ashrafzadeh—to access Intel's highly confidential information, including source code materials. This is a highly improper request that is directly contrary to well-established law in patent cases, the express terms of the N.D. Cal. Model Order, and the positions that Plaintiff's own counsel have taken in other cases.

The default rule in patent cases is that named plaintiffs and inventors are ***not*** permitted access to the defendant's highly confidential information. *See TVIIM, LLC v. McAfee, Inc.*, 2014 WL 2768641, at *2 (N.D. Cal. June 18, 2014) ("[C]ourts have found that a named inventor should not be given access to a patent infringement defendant's confidential information.");

Layne Christensen Co. v. Purolite Co., 271 F.R.D. 240, 252 (D. Kan. 2010) (holding that "Defendant has shown good cause for protection against unqualified access by [an inventor and named plaintiff] to documents designated for 'Attorneys' Eyes Only'…. The protective order will not list [the inventor and named plaintiff] as having access [to] any materials designated as 'Attorneys' Eyes Only'"). The rationale for this rule is simple: having already filed suit against the defendant, a plaintiff given access to highly confidential information of the defendant could—intentionally or even inadvertently—improperly use the defendant's information in the prosecution of a patent, to file a lawsuit, or in some other way outside the context of this lawsuit. *See Tailored Lighting, Inc. v. Osram Sylvania Prods., Inc.*, 236 F.R.D. 146, 149 (W.D.N.Y. 2006) (rejecting plaintiff's request to disclose defendant's technical information to named inventor, even when they were not in direct competition, because "it seems unreasonable to expect that anyone working to further his own scientific and technological interests would be able assuredly to avoid even the subconscious use of confidential information revealed through discovery that is relevant to those interests"); *Tehrani v. Polar Elecs. Inc.*, 2006 WL 8435287, at *3 (C.D. Cal. Nov. 8, 2006) (finding that a plaintiff's patent licensing activity precluded her from accessing highly confidential information noting "[s]uch active licensing renders her the equivalent of a competitor… because she has a financial interest in the underlying technology and thus, the same risk for abuse of discovery exists"); *see also McDavid Knee Guard, Inc. v. Nike USA, Inc.*, 2009 WL 1609395 at *4-5 (N.D. Ill. 2009) (denying patentee's motion to modify stipulated protective order so that the named inventor, who was involved in on-going reissue proceedings of the asserted patent, could have access to technical information obtained from a third-party competitor designated "Highly Confidential").

The N.D. Cal. Model Order adopts this well-established rule. It ***specifically prohibits*** access by any plaintiff to highly confidential information. *See* Ex. 4 at ¶ 2.8 (defining "Highly Confidential – Attorneys' Eyes Only" as "extremely sensitive 'Confidential Information or Items,' disclosure of which to another Party or Non-Party would create a substantial risk of serious harm that could not be avoided by less restrictive means"); *id.* at ¶ 7.3 (excluding parties from list of individuals who may access highly confidential information); *see also Medina*, 2014 WL 3884506, at *2 (N.D. Cal. Model Order provides that highly confidential information "may be disclosed ***only*** to a party's outside counsel, in-house counsel 'who has no involvement in competitive decision-making,' and experts with a need-to-know, along with certain court personnel. *Id.* at ¶ 7.3. Thus, under the plain language of the governing protective order, Dr. Medina—the sole decisionmaker for Plaintiff; indeed, he is Plaintiff—may not have access to highly confidential information." (emphasis added)).

Even Plaintiffs' counsel has taken this same position in the past. When representing defendants, Plaintiffs' counsel have repeatedly sought protective orders that preclude plaintiffs from accessing the defendants' highly confidential information. *See, e.g.*, *I2Z Tech., LLC, v. Microsoft Corp.*, 3:11-cv-1103, Dkt. 36 (D. Or. March 29, 2012) (Klarquist Sparkman, LLP – John Vandenberg) (Paragraph 6.3 of the stipulated protective order prohibits parties other than certain designated in-house counsel from accessing Highly Confidential – Attorneys' Eyes Only information) (Ex. 14); *Walker Digital, LLC v. Fandango, Inc. et. al.*, 1:11-cv-313, Dkt. 88 at ¶ 9 (D. Del. Feb. 14, 2012) (Klarquist Sparkman, LLP – Jeffrey Love) (Paragraph 9 of the stipulated protective order prohibits parties from accessing Highly Confidential – Attorneys' Eyes Only information) (Ex. 13).

Disclosure to Mr. Ashrafzadeh would be particularly inappropriate given his other business activities. Plaintiffs admit that Mr. Ashrafzadeh currently has an interest in Nova Semiconductor, Inc., a company "involved in IP development and licensing" and that has "developed IP around capacitive voltage multiplier." Ex. 5 (July 18 Email from McAndrew to Coviello); (Dkt. 1 at ¶ 15). Plaintiffs admit that Mr. Ashrafzadeh is involved in patent licensing for two companies in this technology area, including Nova Semiconductor, Inc. *Id*. Mr. Ashrafzadeh also is actively working on drafting patent applications relating to microprocessor technology similar to the asserted patent, including temperature measurement circuitry in semiconductor devices. *See* Appl. No. 14/337,627 titled "Load Balancing in Discrete Devices" regarding "an apparatus [that] can include a temperature measurement circuit configured to product a first signal indicating a first operating temperature of a first semiconductor device…." filed by Fairchild Semiconductor on February 5, 2015; Appl. No. 15/676,360 titled "Isolation Between Semiconductor Components" filed by Fairchild Semiconductor on August 14, 2017. This presents an immediate risk of competitive harm to Intel. Mr. Ashrafzadeh could use Intel's information—even inadvertently—in his work at Nova Semiconductor, in licensing discussions, to file another lawsuit, or to draft patent claims to cover Intel's products. Courts have made clear that plaintiffs involved in this type of activity cannot be permitted access to the defendant's highly confidential information. *See e.g.*, *IP Innovation L.L.C. v. Thomson, Inc.*, 2004 WL 771233, at *3 (S.D. Ind. Apr. 8, 2004) (denying request for named inventor to have access to highly confidential documents given his patents in the relevant technology, pending patents in the relevant technology, and his licensing activity); *Tehrani* , 2006 WL 8435287, at *3 (C.D. Cal. Nov. 8, 2006) (noting that plaintiff's licensing activity "renders her the equivalent of a

competitor" in the relevant market "because she has a financial interest in the underlying technology and thus, the same risk for abuse of discovery exists"); *see also Telebuyer*, 2014 WL 5804334, at *6 ("[D]rafting, amending, restructuring, or otherwise participating in reexamination proceedings may constitute 'competitive decision-making,' as contemplated by the Federal Circuit in *Deutsche Bank.*"); *Shared Memory Graphics, LLC v. Apple, Inc.*, 2010 WL 4704420, at *3 (N.D. Cal. Nov.12, 2010) ("Claims may still be restructured in reexamination, and, in a given case, a patent owner may well choose to restructure claims in a manner informed by the alleged infringer's confidential information gleaned from litigation.").

Plaintiffs have not articulated any reason that could possibly overcome this authority. Plaintiffs argue that Mr. Ashrafzadeh needs access to Intel's highly confidential information to "understand" advice of counsel. (Dkt. 65 at 12). This is not a valid basis to permit disclosure of Intel's highly confidential information to Mr. Ashrafzadeh. Courts have made clear that outside counsel can advise clients on strategy without the need to disclose the opposing party's highly confidential information. *See U.S. Steel Corp. v. United States*, 730 F.2d 1465, 1468 (Fed. Cir. 1984) ("In a particular case, e.g., where in-house counsel are involved in competitive decision making, it may well be that a party seeking access should be forced to retain outside counsel or be denied the access recognized as needed."); *Schlafly v. Public Key Partners*, 94-cv-20512, Dkt. 74 at *3-4 (N.D. Cal. July 19, 1995) (protective order that prohibited a pro se plaintiff from receiving certain confidential information was appropriate, even though it required plaintiff to retain counsel or an independent expert to review the information).

Plaintiffs then argue Mr. Ashrafzadeh will abide by the protective order and should therefore receive Intel's highly confidential information. (Dkt. 65 at 12). This again is not

enough. The risk is not just intentional misuse—there is also a risk of unintentional use of information in licensing and patent drafting. *See In re Deutsche Bank Trust Co. Ams.*, 605 F.3d 1373, 1378 (Fed. Cir. 2010) (a party's status as a decision-maker is essential in determining whether that party can access highly confidential information because of the difficulty "for the human mind to compartmentalize and selectively suppress information once learned, no matter how well intentioned the effort may be to do so." (citations omitted)); *Tailored Lighting*, 236 F.R.D. at 149 ("[I]t seems unreasonable to expect that anyone working to further his own scientific and technological interests would be able assuredly to avoid even the subconscious use of confidential information revealed through discovery that is relevant to those interests."). Indeed, if the mere promise of complying with the protective order was enough, every plaintiff in every case would be allowed access to opposing party's highly confidential information. This is not and should not be the law.

Finally, Plaintiffs assert that case law supports their request to disclose Intel's highly confidential information to Mr. Ashrafzadeh. (*See* Dkt. 65 at 12-15). But none of the cases Plaintiffs cite supports their argument. In particular, not one of the cases allows a named plaintiff or an inventor to access an opposing party's highly confidential information. In the *Codexis* case, the court granted a litigant's motion seeking permission to disclose confidential information to an expert, ***not*** highly confidential information to a party in the case. *Codexis, Inc. v. EnzymeWorks, Inc.*, 2017 WL 5992130, at *7 (N.D. Cal. Dec. 4, 2017). In *Merit Industries v. Feuer*, the court allowed a former employee to access certain non-technical documents including "numerous public records such as issued U.S. patents and brochures for dart games" that were not properly designated as highly confidential. 201 F.R.D. 382, 384 (E.D. Pa. 2000). Finally, in

Coca-Cola Bottling Co. of Shreveport v. Coca-Cola Co., 107 F.R.D. 288, 300 (D. Del. 1985), the Court ordered the production of highly confidential trade secrets, but expressly stated that "***it may be advisable to limit the disclosure of the formulae to plaintiffs' trial counsel and independent experts***." (emphasis added).

D. The Prosecution Bar Should Include Plaintiffs' Alternative Definition of "Relevant Technology"

Prosecution bars state that attorneys who access highly confidential information produced by the other side cannot draft or prosecute patent applications relating to a specifically defined "Relevant Technology" for a period of time. Prosecution bars are standard in patent cases in order to prevent counsel from using the information they access during litigation (even inadvertently) to draft patent claims for other clients. *See, e.g.*, *Applied Signal Tech., Inc. v. Emerging Markets Commc'ns, Inc.*, 2011 WL 197811, at *3 (N.D. Cal. Jan. 20, 2011) (prosecution bars are necessary to prevent patent attorneys from using (intentionally or inadvertently) highly sensitive technical information produced by an opposing party to draft patent claims).

The parties agree that a prosecution bar is appropriate in this case. Plaintiffs, however, have moved for relief on two issues relating to the prosecution bar: (1) its temporal scope, and (2) its substantive scope (specifically, the definition of the "Relevant Technology" for which patent prosecution is prohibited). In an effort to compromise, Intel is willing to agree to Plaintiffs' proposed temporal scope: specifically, that the prosecution bar should begin when access to highly confidential information is first received by the affected individual and should end one year after that individual's last access to such material. Ex. 1 at ¶ 8.

The only remaining dispute is thus the definition of the "Relevant Technology" for which patent prosecution is prohibited. Plaintiffs propose two definitions. First, Plaintiffs argue that the Relevant Technology should be "the use of calibration to improve the performance characteristics of voltage regulator circuits for powering integrated circuit and microprocessor chips." Second, they also propose an alternative definition of "circuits for regulating power in microprocessors or other integrated logic circuits." (Dkt. 65 at 8 n.3).

As a compromise, Intel is willing to agree to Plaintiffs' alternative definition of "Relevant Technology." Plaintiffs' first definition—"the use of calibration to improve the performance characteristics of voltage regulator circuits for powering integrated circuit and microprocessor chips"—is far too narrow. This definition requires "the use of calibration," which is a single claim term from the asserted patent (a claim requirement that is missing from Intel's products). Under this proposal, Plaintiffs' counsel could get Intel's information about voltage regulators and power regulation generally, and then prosecute patent applications in these same areas so long as the applications did not specifically relate to "the use of calibration." This proposal would thus effectively eliminate the prosecution bar. Indeed, Plaintiffs have asserted that the patent at issue relates to far broader technology and have demanded a far greater scope of information from Intel. In their Complaint, for example, Plaintiffs argue that the patent relates to: circuits and methods for addressing voltage regulator current sensing variations, voltage droop, manufacturing variations, temperature dependencies, and mismatched phase outputs in a multiphase power regulator (Dkt. 1 at ¶ 2); circuits and methods to properly power a computer processor or integrated circuit chip (*id.*); and increased power efficiencies by allowing power to be more accurately and consistently delivered to the processor (*id.* ¶ 3). Similarly, Plaintiffs

have sought a broad range of documents relating to any functionality of Intel's fully integrated voltage regulator (FIVR)—not simply documents purportedly relating to "calibration." *See, e.g.*, Ex. 16 (Plaintiffs' Request For Production 13) (seeking "All Schematics showing connections to the PCU, unCore, FCM, nonvolatile memory and package I/O with respect to the FIVR components of Intel's products"). Yet under their first proposed definition of "Relevant Technology," Plaintiffs' counsel could receive Intel's highly confidential FIVR information that does not relate to "calibration" and use it to prosecute applications for other clients—the exact thing the prosecution bar is meant to prevent. In addition, the N.D. Cal. Model Order expressly contemplates that the relevant technology is the scope of the production—for relevant technology the parties should "insert subject matter of the invention and of ***highly confidential technical information to be produced***." Ex. 4, ¶ 8 (emphasis added).

Because Plaintiffs will receive Intel information going far beyond any alleged "calibration," the definition of the "Relevant Technology" for which patent prosecution is prohibited should not be so limited. Indeed, because Plaintiffs' counsel will receive Intel confidential information about aspects of Intel's microprocessors significantly beyond even the subject of voltage regulation generally, a much broader definition of Relevant Technology would be appropriate here. But as a compromise position, Intel is willing to agree instead to Plaintiffs' alternative definition—that Relevant Technology be defined as "circuits for regulating power in microprocessors or other integrated logic circuits." (Dkt. 65 at 8 n.3.) Given that Plaintiffs have already indicated that this definition of "Relevant Technology" is acceptable—and given their refusal to meet and confer on this issue—Intel submits that Court should adopt this definition of the Relevant Technology covered by the prosecution bar.

E. Plaintiffs' Attempt to Disclose Intel's Confidential and Highly Confidential Information to Undisclosed Experts Should be Rejected

There is one final issue relating to Plaintiffs' proposed Protective Order that warrants the Court's attention. Intel proposes, as set forth in the N.D. Cal. Model Order, that any party wishing to disclose the other side's confidential or highly confidential information to an expert must first disclose the expert and give the other side an opportunity to object to the expert. Ex. 1 at ¶ 7.3. Plaintiffs have proposed to eliminate this requirement such that Plaintiffs could disclose Intel's most sensitive information—source code, product design documents, financial information, etc.—to undisclosed experts without Intel having any opportunity to object. At paragraph 7.3(d) of their proposed order, Plaintiffs insert a provision stating that any expert "who is not a current officer, director, or employee of a competitor of a Party or anticipated to become one" can review any information Intel produces without being disclosed to Intel and without Intel having a chance to object. Plaintiffs' proposal should be rejected.

Expert disclosure and objection provisions are standard in patent cases. Courts have held that expert disclosure provisions are necessary to ensure that parties can maintain control over the dissemination of their most sensitive information and prevent the disclosure of their information to experts who could misuse the information. *See Wreal LLC v. Amazon.com, Inc.*, 2014 WL 7273852, at *1, *3-4 (S.D. Fla. Dec. 19, 2014) (rejecting plaintiffs' request that the protective order not require it to "disclose the names of nontestifying consulting experts who receive the most-confidential type of discovery"); *In re Neubauer*, 173 B.R. 505, 508 (D. Md. 1994) (affirming bankruptcy court's issuance of protective order that requires identification of consulting experts to allow producing party "to object to [receiving party's] disclosure of its

confidential information provided in discovery…. Such a provision is necessary to assure no commercial harm to [producing party] and does not inhibit [receiving party's] discovery rights…."). Consistent with this standard practice, expert disclosure provisions have been included in protective orders in multiple prior cases involving Intel, including cases in this District. *See Memory Integrity, LLC v. Intel Corporation*, 3:15-cv-262, Dkt. 92 at 11, 21-23 (D. Or. June 3, 2015) ("Prior to disclosing any Protected Material to any [Person], the Party seeking to disclose such information shall provide the Producing Party with written notice . . . Within ten (10) days of receipt of the disclosure of the Person, the Producing Party or Parties may object in writing to the Person for good cause.") (Ex. 10); *Hangartner v. Intel Corp.*, 3:14-cv-141, Dkt. 68 at 10-11 (D. Or. July 17, 2014) ("[T]he Receiving Party must provide written notice to all counsel of record no less than ten (10) days prior to any disclosure of . . . Protected Documents. . . . If, within ten (10) calendar days after receipt of the notice, counsel for the Producing Party objects to such intended disclosure, the Receiving Party shall not make such disclosure until such objection is resolved by agreement of the parties or by a ruling of the Court on a motion by the Producing Party.") (Ex. 11); *SemCon Tech, LLC v. Intel Corp.*, 3:13-cv-99, Dkt. 79 at 7 (D. Or. April 12, 2013) ("A Party that makes a written notice and provides the information specified in the preceding paragraph may disclose the Protected Matters to the identified expert or consultant unless, within ten (10) business days of the written notice . . . the Producing Party objects in writing.") (Ex. 15). In fact, Plaintiffs' counsel have themselves repeatedly sought protective orders that require expert disclosure and give the parties an opportunity to object to proposed experts. *See Walker Digital LLC, v. Fandango, Inc. et. al.*, 1:11-cv-313, Dkt. 88 at 13 (D. Del. Feb. 14, 2012) (Klarquist Sparkman, LLP – Jeffrey Love) (highly confidential information may

be disclosed to "Actual or potential independent experts or consultants … whose identity, curriculum vitae, and litigation consulting or expert work … is provided to the party whose Protected Matters are to be disclosed for purposes of their making a reasonable objection prior to any disclosure of Protected Matters;") (Ex. 13); *I2Z Technology, LLC, v. Microsoft Corporation*, 3:11-cv-1103, Dkt. 36 at 14 (D. Or. March 29, 2012) (Klarquist Sparkman, LLP – John Vandenberg) (highly confidential information may be shown to "Experts of the Receiving party … as to whom the procedures set forth in paragraph 6.5(a) [governing disclosure and objection], below, have been followed;") (Ex. 14).

Plaintiffs argue that their attempt to eliminate the expert disclosure procedure is supported Footnote 7 of the N.D. Cal. Model Order. (Dkt. 65 at 17). That note states that an "alternative" to the Model provision requiring expert disclosure is a provision that would allow a party to provide materials to an undisclosed expert who is not a competitor to a party. There is no basis to use this "alternative" in a case like this one, involving production of highly sensitive product design information (including source code) that discloses the exact blueprint for billions of dollars of industry-leading microprocessors. To the contrary, the case law cited above, prior cases involving Intel, and Plaintiffs' counsel's own prior practice show that Plaintiffs' provision is not appropriate.

Plaintiffs also argue that their proposal removes the notice requirement only for experts who do not work for competitors. (Dkt. 65 at 17). But even proposed experts who do not work for competitors may be objectionable. For example, courts have held that experts who had a prior confidential relationship with an adverse party may be disqualified—even if they do not work for a competitor. *See, e.g., Oracle Corp. v. DrugLogic, Inc.*, 2012 WL 2244305, at *6

(N.D. Cal. June 15, 2012) (an expert should generally be disqualified if "the [party] had a confidential relationship with the expert and (2) the [party] disclosed confidential information to the expert that is relevant to the current litigation."); *see also Auto-Kaps, LLC v. Clorox Co.*, 2016 WL 1122037, at *4 (E.D.N.Y. Mar. 22, 2016) (expert disqualified because he "was likely exposed throughout his consultancy to the goals and priorities [of the adverse party], which [he] may inadvertently use to determine whether the [accused technology] met certain claim limitations"); *Pellerin v. Honeywell Int'l Inc.*, 2012 WL 112539, at *1 (S.D. Cal. Jan. 12, 2012) (disqualifying former employee who was responsible for technology design). Further, under Plaintiffs' proposal, Plaintiffs would be able to unilaterally decide who is a "competitor" to Intel. Intel should have the opportunity to address whether an expert works for a competitor. Indeed, because of the complexity of Intel's business, Plaintiffs may not even know a particular company competes with part of Intel's business.

For each of these reasons, Plaintiffs' proposal to eliminate the expert disclosure provision should be rejected.[3]

[3] The Court should also reject Plaintiffs' alternative proposal to enter the D. Oregon model two-tier Protective Order. (Dkt. 65 at 18). The model does not include any source code or prosecution bar provisions, and Plaintiffs have made no argument as to why that order should be adopted in this case.

IV. CONCLUSION

Plaintiffs' motion is a motion that never should have been filed. Plaintiffs failed to properly meet and confer—needlessly burdening the Court with issues that are not in dispute—and Plaintiffs have taken extreme positions that would put Intel's highly confidential information at risk, that are inconsistent with typical practice in patent cases (including the N.D. Cal. Model Order), and that are inconsistent with Plaintiffs' counsel's own practices in other cases. Intel respectfully requests that Plaintiffs' motion be denied, that the Court enter Intel's proposed protective order (Exhibit 1), and that Intel be awarded its costs in opposing this motion.

DATED: August 8, 2018

MARKOWITZ HERBOLD PC

By: */s/ Renée E. Rothauge*

Renée E. Rothauge, OSB #903712
ReneeRothauge@MarkowitzHerbold.com
(503) 295-3085

WILMER CUTLER PICKERING HALE AND DORR LLP
Michael J. Summersgill (*pro hac vice*)
Jordan L. Hirsch (*pro hac vice*)
Todd C. Zubler (*pro hac vice*)

Attorneys for Defendant and Counterclaim Plaintiff Intel Corporation